

IN THE UNITED STATES DISTRICT COURT FOR
THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF A
SAMSUNG CELLULAR TELEPHONE, MEID
HEX A0000048D94ECD, USING MOBILE
NUMBER 724-317-3440.

Magistrate No.

16 486 M

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Terrence R. Sweeney, Special Agent, Federal Bureau of Investigation, United States Department of Justice, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, a cellular telephone, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent ("SA") of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and have been so employed for twenty (20) years. Since March of 2008, I have been assigned to the Mon Valley Resident Agency of the FBI's Pittsburgh Division. During my time with the FBI, I have been assigned to investigative units dealing with organized crime, drug trafficking, gangs, and violent crimes. During my training at the FBI Academy in Quantico, Virginia, I received extensive training in a variety of investigative and legal matters, including the topics of Fourth Amendment searches and the constitutional requirements for the interception of telephone communications. I have been involved in many narcotics-related arrests and the service of many narcotics-related search warrants. I have

handled cooperating sources of information who were involved in narcotics acquisition and/or trafficking. In addition, I have reviewed thousands of communications between drug traffickers as a result of my participation in multiple wiretap investigations. As a result of my narcotics-related training and experience, I am familiar with the methods and language used to distribute narcotics, to launder proceeds, and to operate drug-trafficking conspiracies. I have experience conducting surveillance, analyzing telephone records, interviewing witnesses, executing search and arrest warrants, and other investigative techniques. The investigations in which I have participated have resulted in the arrest and prosecution of individuals who have smuggled, received, and distributed controlled substances, including heroin and cocaine. I have participated in several investigations in which court-authorized wire and electronic interceptions were utilized. I have provided trial testimony in federal court, subject to cross-examination, about how such wiretap investigations are conducted. Based on my training and experience, I am aware that it is common practice for drug traffickers who desire to insulate themselves from detection by law enforcement to routinely utilize multiple telephones, counter surveillance, false or fictitious identities, and coded communications to communicate with their customers, suppliers, couriers, and other conspirators. It is not unusual for drug traffickers to initiate or subscribe such phone or phone device services under the names of other real or fictitious people. Moreover, it is now a very common practice for drug traffickers to utilize all communication features of their telephones, most notably the voice call and text message features, nearly simultaneously to communicate with their conspirators.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched consists of one Samsung cellular telephone, MEID HEX A0000048D94ECD, using mobile number 724-317-3440, hereinafter the **Target Telephone**.

5. The applied-for warrant would authorize the forensic examination of the **Target Telephone** for the purpose of identifying electronically stored data particularly described in Attachment B.

6. There is probable cause to believe that the **Target Telephone** contains evidence of violations of 18 U.S.C. §§ 2113(a) and 2113(d). In particular:

a. The **Target Telephone** was recovered on March 18, 2016, from a white Chevrolet Malibu driven by Aaron HUEY, who drove it to a meeting with agents conducting this investigation. The car was registered to HUEY's girlfriend, Marcel TANSMORE, who consented to the search of the vehicle. Agents used the mobile number listed above for the **Target Telephone** to communicate with HUEY over the **Target Telephone** in order to arrange the meeting at which the search of the car occurred.

b. On the same day, March 18, 2016, your affiant believes that HUEY attempted to rob the PNC Bank in Charleroi, Pennsylvania. A witness in a vehicle near the bank saw a male wearing a surgical-type mask and gloves approach the doors of the bank and attempt to enter, but the bank doors were locked. The witness identified the license plate as Pennsylvania registration HWG-4108, which records show belongs to the same white Chevrolet Malibu driven by HUEY and owned by TANSMORE. A review of surveillance video from surrounding locations shows a white Chevrolet Malibu approaching the PNC Bank shortly before the attempted robbery.

c. Two days earlier, a PNC Bank in Carmichaels, Pennsylvania was robbed a male wearing a surgical-type mask and gloves, who threatened the teller with what appeared to be a handgun. A witness outside the bank saw the robber leave the bank and drive away in a white Chevrolet Malibu, and captured the episode on a cell phone video reviewed by your affiant. The Malibu appears similar to the one owned by TANSMORE and driven by HUEY.

d. On December 11, 2015, the Frick Tri-County Federal Credit Union was robbed. A male wearing a surgical-type mask handed the teller a note demanding money, and saying no one would get shot. A witness saw the robber drive away in a silver Mercedes sedan. At that time, HUEY was driving a silver Mercedes sedan in the name of his friend, Jeffrey THOMPSON, who agreed to place the sedan in his own name because of HUEY's poor credit. THOMPSON told your affiant that HUEY was driving the silver Mercedes around December 11, 2015, and that it was repossessed in March 2016.

e. Your affiant obtained cell-site location information for the **Target Telephone** with an order issued by Magistrate Judge Maureen Kelly at MJ 16-268 on March 24, 2016. I am aware as a result of information provided by law enforcement that those engaged in unlawful activity often rely heavily on their cellular telephones and related communications. These communications, in the form of telephone calls, voice messages, sms text messages, and other similar communications, cause their cellular telephones to emit and receive electronic signals to and from cellular telephone company cell towers. The cellular telephone company records of the interaction between these signals and the cell towers used to receive and send them can indicate the general geographic location of the individual using a particular cellular telephone at a particular moment in time. The data shows that the **Target Telephone** connected to a cellular tower east of Carmichaels, PA at 11:49 a.m. and west of Carmichaels, PA at 11:50

a.m. on March 16, 2016. At 12:27 p.m., the PNC Bank in Carmichaels, PA was robbed by the person your affiant believes to be HUEY, who got into the white Malibu and who was using the **Target Telephone**. The cell-site location data reviewed by your affiant shows no other connections to Carmichaels, PA-area cellular towers on other days, and it shows no other calls by the **Target Telephone** close in time to the robbery. HUEY lives in Donora, PA, which is in Washington County; Carmichaels, PA is in Greene County.

f. Your affiant also reviewed cell-site location information for the **Target Telephone** for March 18, 2016, the day of the attempted robbery. At 4:32 p.m., the **Target Telephone** connected to a cellular tower in North Charleroi, PA. At 4:35 p.m., the witness reported the attempted robbery at the PNC Bank in Charleroi, PA.

g. I am aware that the Supreme Court has recognized that probable cause to support a search warrant exists when there is a fair probability that the location or item to be searched contains evidence or information that would be helpful in prosecuting an individual, establishing motive, impeaching a witness, rebutting a defense, or in otherwise securing a proper conviction. *See Messerschmidt v. Millender*, 132 S.Ct. 1235, 1247-49 (2012). The use of the **Target Telephone** close in time to the robberies on March 16 and 18, 2016, leads your affiant to believe that the **Target Telephone** will contain evidence relevant to the commission of the offenses listed above. In particular, records on the **Target Telephone** could confirm the nature of HUEY's communications around the time of the robberies.

7. The **Target Telephone** is currently in the lawful possession of the Federal Bureau of Investigation.

8. In my training and experience, I know that the **Target Telephone** has been stored in a manner in which their contents are, to the extent material to this investigation, in

substantially the same state as they were when the **Target Telephone** first came into the possession of the FBI.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

9. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

10. There is probable cause to believe that things that were once stored on the **Target Telephone** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of

how a computer has been used, what it has been used for, and who has used it.

To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

Forensic Evidence: Deleted Files, User Attribution

11. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Target Telephone** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Target Telephone** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to

draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Target Telephone** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

13. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

14. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **Target Telephone** described in Attachment A to seek the items described in Attachment B.

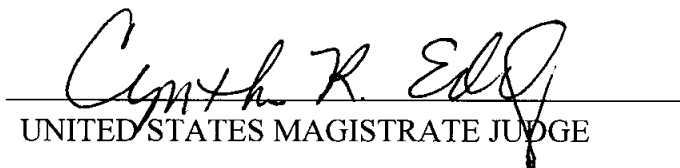
Respectfully submitted,

A handwritten signature in black ink, appearing to read "T.R. Sweeney", written over a horizontal line.

Terrence R. Sweeney
Special Agent, Federal Bureau of
Investigation

Subscribed and sworn to before me

on 5/10/16

A handwritten signature in black ink, appearing to read "Cynthia R. Edg", written over a horizontal line.
UNITED STATES MAGISTRATE JUDGE